CHAPTER 11

Cisco TrustSec ファイバ チャネル リンク暗号化の設定

この章では、Cisco TrustSec ファイバ チャネル（FC）リンクの暗号化機能の概要を示し、スイッチ間にリンクレベルの暗号化を設定する方法について説明します。

この章では、次の事項について説明します。

- 「Cisco TrustSec FC リンク暗号化の概要」（P.11-1）
- 「注意事項と制限」（P.11-2）
- 「Cisco TrustSec ファイバ チャネル リンク暗号化の設定」（P.11-2）
- 「ESP の設定」（P.11-4）
- 「Cisco TrustSec ファイバ チャネル リンク暗号化設定の確認」（P.11-6）

Cisco TrustSec FC リンク暗号化の概要

Cisco TrustSec FC リンク暗号化は、Fibre Channel-Security Protocol（FC-SP）の拡張機能であり、既存の FC-SP アーキテクチャを使用してトランザクションの整合性と機密保持を実現します。セキュリティを保ち、望ましくないトラフィック傍受を防止するため、ピア認証機能に暗号化が追加されました。ピア認証は、Diffie-Hellman（DH）Challenge Handshake Authentication Protocol（DHCHAP）プロトコルを使用した FC-SP 標準に従って実装されます。

（注） Cisco TrustSec FC リンク暗号化は現在、Cisco MDS スイッチ間に限りサポートされています。この機能は、カプセル化セキュリティ ペイロード（ESP）プロトコルをサポートしていないソフトウェア バージョンにダウングレードするとサポートされなくなります。

ここで説明する内容は、次のとおりです。

- 「サポートされているモジュール」（P.11-1）
- 「Cisco TrustSec FC リンク暗号化に関する用語」（P.11-2）
- 「AES 暗号化のサポート」（P.11-2）

サポートされているモジュール

次のモジュールは、Cisco TrustSec FC リンク暗号化機能に対応しています。

- 1/2/4/8 Gbps 24 ポート ファイバ チャネル スイッチング モジュール（DS-X9224-96K9）

- 1/2/4/8 Gbps 48 ポート ファイバ チャネル スイッチング モジュール（DS-X9248-96K9）
- 1/2/4/8 Gbps 4/44 ポート ファイバ チャネル スイッチング モジュール（DS-X9248-48K9）

Cisco TrustSec FC リンク暗号化に関する用語

この章では、次に示す Cisco TrustSec FC リンク暗号化関連の用語を使用します。

- ガロア カウンタ モード（GCM）：機密保持とデータ発信元認証を行う操作のブロック暗号モード。
- ガロア メッセージ認証コード（GMAC）：データ発信元認証だけを行う操作のブロック暗号モード。GCM の認証限定バリアントです。
- セキュリティ アソシエーション（SA）：セキュリティ認定証を処理し、それらの認定証をスイッチ間にどのように伝播するかを制御する接続。SA には、salt やキーなどのパラメータが含まれます。
- キー：フレームの暗号化および復号化に使用する 128 ビットの 16 進数字列。デフォルト値は 0 です。
- Salt：暗号化および復号化の際に使用する 32 ビットの 16 進数字列。適切な通信を行うには、接続の両側に同じ salt を設定する必要があります。デフォルト値は 0 です。
- セキュリティ パラメータ インデックス（SPI）番号：ハードウェアに設定される SA を識別する 32 ビットの数字。有効な範囲は 256 ～ 4,294,967,295 です。

AES 暗号化のサポート

Advanced Encryption Standard（AES）は、ハイレベルなセキュリティを実現する対称暗号アルゴリズムであり、さまざまなキー サイズを受け入れることができます。

Cisco TrustSec FC リンク暗号化機能は、セキュリティ暗号用に 128 ビットの AES をサポートし、インターフェイスに AES-GCM または AES-GMAC のいずれかをイネーブルにします。AES-GCM モードではフレームの暗号化と認証が可能であり、AES-GMAC では 2 つのピア間で送受信されるフレームの認証だけが可能です。

注意事項と制限

ここでは、Cisco TrustSec FC リンク暗号化に関する注意事項を示します。

- Cisco TrustSec FC リンク暗号化が MDS スイッチ間だけでイネーブルであることを確認します。この機能は、E ポートまたは ISL だけでサポートされており、MDS 以外のスイッチを使用している場合はエラーが発生します。
- 接続にかかわるピアの設定が同一であることを確認します。設定に相違があると、「port re-init limit exceeded」というエラー メッセージが表示されます。
- スイッチ インターフェイスの入力および出力ハードウェアに SA を適用する前に、インターフェイスが admin shut モードであることを確認します。

Cisco TrustSec ファイバ チャネル リンク暗号化の設定

ここで説明する内容は、次のとおりです。

- 「Cisco TrustSec FC リンク暗号化のイネーブル化」（P.11-3）

- 「セキュリティ アソシエーションの設定」（P.11-3）
- 「セキュリティ アソシエーション パラメータの設定」（P.11-3）

Cisco TrustSec FC リンク暗号化のイネーブル化

Cisco MDS 9000 ファミリのすべてのスイッチの FC-SP 機能と Cisco TrustSec FC リンク暗号化機能は、デフォルトでディセーブルになります。

ファブリック認証および暗号化用のコンフィギュレーション コマンドおよび確認コマンドにアクセスするには、FC-SP 機能をイネーブルにする必要があります。この機能をディセーブルにすると、関連するすべての設定が自動的に廃棄されます。

セキュリティ アソシエーションの設定

スイッチ間で暗号化を実行するには、セキュリティ アソシエーション（SA）を設定する必要があります。暗号化を実行するには、管理者があらかじめ手動で SA を設定する必要があります。SA には、キーや salt など、暗号化に必要なパラメータが含まれます。スイッチには、最大 2000 の SA を設定できます。

（注）　Cisco TrustSec FC リンク暗号化は現在、on モードと off モードの DHCHAP だけでサポートされています。

セキュリティ アソシエーション パラメータの設定

手順の詳細

DCNM-SAN を使用してキーや salt などの SA パラメータを設定する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] を展開し、[FC-SP (DHCHAP)] を選択します。
[Information] ペインに、FC-SP の設定が表示されます。

ステップ 2　[SA] タブをクリックします。
各スイッチの SA パラメータが表示されます。

ステップ 3　[Create Row] アイコンをクリックします。
[Create SA Parameters] ダイアログボックスが表示されます。

ステップ 4　暗号化を実行するスイッチを選択します。

ステップ 5　SP の値を選択します。有効な範囲は 256 ～ 65536 です。

ステップ 6　salt の値を入力します。または、[Salt Generator] ボタンをクリックして値を選択します。

ステップ 7　キーの値を入力します。または、[Key Generator] ボタンをクリックして値を選択します。

ステップ 8　[Create] ボタンをクリックして変更内容を保存します。

Device Manager を使用してキーや salt などの SA パラメータを設定する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] を選択し、[FC-SP] を選択します。

[FC-SP] 設定ダイアログボックスが表示されます。

ステップ 2　[SA] タブをクリックします。

各スイッチの SA パラメータが表示されます。

ステップ 3　[Create] ボタンをクリックして、新しいパラメータを作成します。

[Create FC-SP SA] ダイアログボックスが表示されます。

ステップ 4　SP の値を選択します。有効な範囲は 256 ～ 65536 です。

ステップ 5　salt の値を入力します。または、[Salt Generator] ボタンをクリックして値を選択します。

ステップ 6　キーの値を入力します。または、[Key Generator] ボタンをクリックして値を選択します。

ステップ 7　[Create] ボタンをクリックして変更内容を保存します。

ESP の設定

（注）　インターフェイスの入力および出力ハードウェアに SA を適用するには、インターフェイスが admin shut モードである必要があります。

（注）　ESP モードが設定されるのは、入力または出力ハードウェアに SA が設定されている場合だけです。SA が設定されていない場合は、ESP がオフになり、カプセル化は行われません。

（注）　ポートを設定した後で ESP モードを変更した場合は、変更がシームレスでないため、常にポートのフラップが必要です。ただし、設定は拒否されません。

手順の詳細

ESP を設定する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] を展開し、[FC-SP (DHCHAP)] を選択します。

[Information] ペインに、FC-SP の設定が表示されます。

ステップ 2　[ESP Interfaces] タブをクリックします。

各スイッチのインターフェイスの詳細が表示されます。

ステップ 3　[Create Row] アイコンをクリックします。

[Create ESP Interfaces] ダイアログボックスが表示されます。

ステップ 4　暗号化を実行するスイッチを選択します。

ステップ 5　選択したスイッチのインターフェイスを入力します。

ステップ 6　暗号化用に適切な ESP モードを選択します。

ステップ 7　暗号化用に適切な出力ポートを入力します。

ステップ 8　暗号化用に適切な入力ポートを入力します。

ステップ 9　[Create] ボタンをクリックして変更内容を保存します。

Device Manager を使用して ESP を設定する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] を展開し、[FC-SP] を選択します。

[FC-SP] 設定ダイアログボックスが表示されます。

ステップ 2　[ESP Interfaces] タブをクリックします。

各スイッチのインターフェイスの詳細が表示されます。

ステップ 3　[Create] をクリックします。

[Create FC-SP ESP Interfaces] ダイアログボックスが表示されます。

ステップ 4　暗号化用にスイッチのインターフェイスを入力します。または、選択したスイッチに使用できるインターフェイスから値を選択することもできます。

ステップ 5　暗号化用に適切な ESP モードを選択します。

ステップ 6　暗号化用に適切な出力ポートを入力します。

ステップ 7　暗号化用に適切な入力ポートを入力します。

ステップ 8　[Create] ボタンをクリックして変更内容を保存します。

ESP ウィザードを使用した ESP の設定

ESP ウィザードを使用して、スイッチ間のリンクレベル暗号化を設定できます。このウィザードを使用して、既存の スイッチ間リンク（ISL）をセキュアな ISL として設定することも、既存のセキュアな入力 SPI および出力 SPI を編集することもできます。

手順の詳細

ESP ウィザードを使用して ESP を設定する手順は、次のとおりです。

ステップ 1　[Tools] > [Security] > [FC-SP ESP Link Security] を右クリックして、DCNM-SAN から ESP ウィザードを起動します。

ステップ 2　保護する、またはセキュリティを編集する適切な ISL を選択します。

（注）　FC-SP ポート モードが有効で、ESP 対応のスイッチまたはブレードで使用可能な ISL だけが表示されます。

ステップ 3　新しいセキュリティ アソシエーション（SA）を作成します。

スイッチごとに新しい SA を作成することも、既存の SA を使用することもできます。既存の SA を表示するには、[View Existing SA] をクリックします。

（注）　既存の SA のリストには、1 台のスイッチに対する既存の SA がすべて表示されます。ウィザードは、スイッチのペアに共通の SA が存在する場合だけ稼働します。[Next] ボタンを選択すると、この要件がチェックされ、スイッチのペアに共通の SA が存在しない場合は警告メッセージが表示されます。このウィザードを実行するには、スイッチのペアに共通の SA を作成する必要があります。

ステップ 4　選択した ISL に関する出力ポート、入力ポート、および ESP モードを指定します。

セキュリティで保護された ISL の場合、スイッチのペアに共通する SA の SPI が出力ポートと入力ポートに自動入力されます。

この場合、モードはディセーブルになります。セキュリティで保護された ISL のモードは編集できません。

（注）　選択した ISL がイネーブルであれば、既存の ESP 設定を変更できます。

ステップ 5　設定を確認します。

ステップ 6　[Finish] ボタンをクリックして、ESP の設定を開始します。ステータス カラムに設定のステータスが表示されます。

スイッチのキーの変更

入力および出力ポートに SA を適用した後は、キーの設定を定期的に変更してください。トラフィックの中断を避けるには、キーを順番に変更する必要があります。

Cisco TrustSec ファイバ チャネル リンク暗号化設定の確認

DCNM-SAN または Device Manager では、**show** コマンドを使用して Cisco TrustSec FC リンク暗号化機能の情報を表示できます。

これらのコマンドの出力に表示される各フィールドの詳細については、『*Cisco MDS 9000 Family Command Reference*』を参照してください。

ここでは、次の内容について説明します。

- 「FC-SP インターフェイス統計情報の表示」（P.11-6）
- 「Device Manager を使用した FC-SP インターフェイス統計情報の表示」（P.11-7）

FC-SP インターフェイス統計情報の表示

DCNM-SAN を使用して、カプセル化セキュリティ ペイロード（ESP）プロトコルのセキュリティ パラメータ インデックス（SPI）の不一致や、インターフェイスのカプセル化セキュリティ ペイロード プロトコルの認証エラー情報を示す統計データを表示できます。

インターフェイスの ESP 統計情報を表示する手順は、次のとおりです。

ステップ 1　[Interfaces] > [FC Physical] を展開し、[FC-SP] を選択します。
[Information] ペインに、FC-SP の設定が表示されます。

ステップ 2　[FC-SP] タブをクリックします。
[Information] ペインに FC-SP 統計情報が表示されます。

ステップ 3　[Refresh] ボタンをクリックして、統計データをリフレッシュします。

Device Manager を使用した FC-SP インターフェイス統計情報の表示

Device Manager を使用してインターフェイスの ESP 統計情報を表示する手順は、次のとおりです。

ステップ 1　[Security] > [FC Physical] を展開し、[FC-SP] を選択します。
[Information] ペインに、FC-SP の設定が表示されます。

ステップ 2　[Statistics] タブをクリックします。
[Information] ペインに統計情報が表示されます。

ステップ 3　[Refresh] ボタンをクリックして、統計データをリフレッシュします。